Adapted Privacy Impact Assessment

Android Developer Applications

January 31, 2013

Contact

Departmental Privacy Office
U.S. Department of the Interior
1849 C Street NW
Mail Stop MIB-7456
Washington, DC 20240
202-208-1605
DOI_Privacy@ios.doi.gov

One Privacy Impact Assessment (PIA) may be prepared to cover multiple websites or applications that are functionally comparable as long as agency or bureau practices are substantially similar across each website or application. However, any use of a third-party website or application that raises distinct privacy risks requires a complete PIA exclusive to the specific website or application. Department-wide PIAs must be elevated to the OCIO for review and approval.

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

Mobile devices have increasingly become a primary tool for transmitting and receiving digital information. Android is an operating system for mobile devices such as smartphones and tablet computers and is owned by Google, Inc. Android supports the development of applications by third parties, and thousands of developers have created applications for the Android operating system. In part due to the availability and variety of applications, Android has become the world's leading smartphone platform, with Android installed on over 331 million mobile devices worldwide as of June 2012.

Presidential Memorandum, "Building a 21st Century Digital Government", dated May 23, 2012 (http://www.whitehouse.gov/sites/default/files/uploads/2012digital_mem_rel.pdf), requires Federal agencies to provide more efficient and coordinated digital service delivery. Among other directives, the memorandum instructs Departmental and Agency leaders to implement plans to make full use of mobile technologies in the dissemination of information to the public.

In accordance with the Presidential Memorandum, and to disseminate information to the public and enhance communication, to foster and share ideas, promote public participation and collaboration, and increase government transparency, DOI will design and distribute various Android applications. While the content available through DOI Android applications will also be available through other sources, such as various social media sites used by DOI, Android applications will provide content through the increasingly important mobile device channel, thereby improving public access to relevant content in real-time.

DOI is currently planning to deploy two types of Android applications - content delivery applications and scientific data collection applications.

Content Delivery Applications. DOI's content delivery Android applications will disseminate information to the public, including text, images, audio and video. While these applications will be largely unidirectional in nature, Android developer tools include standard application programming interfaces (APIs) that permit the integration of instant messaging, email, discussion threads, and other types of interactive tools, which DOI may utilize to facilitate feedback and public interaction related to the distributed content. DOI's content delivery applications are designed to maximize the dissemination of useful data to the public and will include information about DOI facilities and locations, press releases and news updates, special events, and information about games such as geocaching. DOI is currently planning to develop several applications to issue

information such as press releases and information about DOI events, which will include relevant photos and videos. DOI will also develop applications to provide information about specific DOI sites, such as national parks, monuments and wildlife refuges, including self-guided tours of those sites.

Scientific Data Collection Applications. DOI will design and distribute Android applications that gather data and information from the public for scientific purposes, or otherwise collect useful data that can be applied in furtherance of DOI's mission and initiatives. The data collected will primarily be scientific and will not contain personally identifiable information (PII).

The potential value in using mobile devices for scientific data collection can be seen in two statistics related to the 2011 Virginia earthquake, which damaged numerous structures in the Washington, DC area and was felt as far north as Quebec City, Quebec: (1) Within four hours of the quake, USGS' "Did you feel it?" earthquake reporting website received over 100,000 submissions related to the quake, and (2) Twitter users in New York City and Boston reported that they received tweets about the earthquake from Twitter users in Virginia and Washington DC 15 to 30 seconds before feeling the quake itself (http://en.wikipedia.org/wiki/2011_Virginia_earthquake).

Mobile device technology is evolving rapidly and the number of mobile device users continues to grow. DOI will develop additional Android applications as new opportunities to exploit the powerful data dissemination and collection opportunities of mobile technologies are identified. To the extent that these applications collect data that is provided voluntarily and in a manner totally transparent to the user, and do not raise distinct privacy risks not discussed in this PIA, the applications will be covered by this PIA. Otherwise, a separate PIA will be conducted for the use of the specific application.

Primary responsibility for the creation and dissemination of DOI Android applications will be held by the Department's bureaus and offices. DOI's Office of Communications will be responsible for providing guidelines to all bureaus and offices defining baseline requirements for all such applications before they can be released to any Android store for public distribution. DOI bureaus and offices that create and disseminate mobile applications will be responsible for ensuring their mobile applications are appropriate for public distribution and in keeping with all applicable DOI rules and policies. All DOI mobile applications will comply with applicable laws, regulations, and DOI privacy, security and social media policies.

DOI's Android applications are developed and distributed through DOI's web site, as well as the official Android application store, known as Google Play. Google Play can be accessed directly through the Google Play application on mobile devices running updated versions of Android, or through the Google Play web site (https://play.google.com/).

The use of Google Play, including purchasing and downloading applications from Google Play, is governed by Terms of Service that are specific to the user's country. Users in the United States are governed by the Google Play Terms of Service, which incorporate Google's universal Terms of Service and adds additional terms specific to Google Play and the applications available through Google Play, and Google Play Business and Program Policies. Pursuant to Google's universal Terms of Service and Privacy Policy, which apply a uniform set of terms across virtually all of Google's web sites and applications, information provided by users of one Google service, including

PII, may be combined or integrated into other Google services. Google users can adjust their privacy settings and exhibit control over some of the personal information tied to their Google account and with whom that information is shared.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities for the use of the third-party website or application?

Executive Order 13571, Streamlining Service Delivery and Improving Customer Service, April 27, 2011; Presidential Memorandum, "Building a 21st Century Digital Government", May 23, 2012; Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; the Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 U.S.C. 1401; OMB Circular A-130; 210 Departmental Manual 18; and 110 Departmental Manual 5.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

The amount and type of PII that will be made available to DOI varies by application, as described below.

Content Delivery Applications

Although DOI's content delivery applications will be largely unidirectional in nature, Android developer tools include standard application programming interfaces (APIs) that permit the integration of instant messaging, email, discussion threads, and other types of interactive tools, which DOI may utilize to facilitate feedback and public interaction in support of the DOI mission.

DOI does not expect to receive a large volume of information about individuals through the use of the content delivery applications, and most of the PII received by DOI will be obtained through voluntary and transparent user interaction via the interactive API tools described above. PII that may become available through user interactions using content delivery applications may include name, username, email address or other personal information provided by the user. Data provided by users of these tools will be initially held by Google and passed to DOI when necessary for proper operation of the application. DOI may also use this information as needed to provide responses to users or supply requested information, but will not otherwise request or collect PII.

Scientific Data Collection Applications

DOI will also design and distribute Android applications to collect data and information from the public for scientific purposes or otherwise in furtherance of DOI's mission and

supporting initiatives. Most of the information collected will not be PII, and DOI will take steps to minimize the collection, use, and storage of any PII from individuals.

The PII that DOI may collect includes basic contact information, such as name and email address. This information will be collected where the ability to contact a user for a follow up discussion might yield additional benefits and contact information will be collected only with explicit user consent.

DOI's scientific data collection applications may also use a unique anonymous personal identifier that can be used to weed out "nuisance" submitters or individuals, or automated responders that are deemed unreliable. Applications will utilize a hash algorithm to create a unique alphanumeric identifier for each user based on the user's Google ID or username. The anonymous ID generated by the hash algorithm can be used to block users that submit obviously false reports or spam. The use of industry standard one-way hashing methods will make reversal of the hash (to reveal the original username) difficult. Therefore, while the hashed ID will be unique, it will not be identifiable to a specific individual. In all cases, the initial collection will utilize Google IDs and the hash will be performed immediately upon collection on Google's servers. DOI will be able to receive the hashed values, but will not receive the Google ID or username.

In addition, DOI's scientific data collection applications may collect geolocation information, as described below.

Geolocation Information

DOI will also utilize geolocation APIs in some of its content delivery and scientific data collection applications. DOI will only utilize geolocation APIs where doing so will significantly improve DOI's ability to provide specific, relevant content to users where it will permit DOI to provide a significant benefit to the public and only after a user has been prompted to allow the collection of such data per request.

In many cases, DOI will not receive specific user location data. For instance, a self-guided tour of a national monument will utilize a geolocation API that will result in a user's location data being transmitted to Google's servers. By default, Android mobile devices internally track the device's location and will transmit location data back to Google pursuant to application program instructions; users have the option to turn off the location tracking feature for their device. Once the location data is received by Google, the specific location coordinates will trigger the transmission of specific data back to the user, such as text or audio describing a specific point of interest. In this case, DOI will never receive the location coordinates.

DOI may receive aggregate, anonymous location information for the purpose of tracking general trends. As an example, with a self-guided tour application, this would permit DOI to identify the popularity of certain sites at a national park.

In some cases, geolocation information will be collected by DOI, but will not be collected along with any other PII that could identify the individual user. In other cases, applications such as the endangered species spotter will collect geolocation information

along with additional PII, such as contact information, that can be used for follow up communications.

Registration with Google

In order to use a DOI Android application, a user must have an Android-equipped device. Most Android users utilize a Google account in order to obtain applications from Google Play. Google account registration requires users to provide their first and last name, a username which is used to generate an email address ([username]@gmail.com), password, date of birth, gender, and mobile phone number. All registration information is held by Google and is not provided to DOI. While registration with Google is a prerequisite for downloading Android applications from Google Play or the DOI App Store, the creation and dissemination of Android applications by DOI is not expected to have any impact on the decision of individuals to purchase Android-equipped devices and register for Google accounts. Therefore, DOI's use of Android applications will not result in the collection of registration information from additional users.

Ratings of Applications

Android users are provided with the opportunity to rate and review Android applications through Google Play; ratings and reviews can be viewed by other users through the Google Play Android application or web site. If a user submits a rating or review of a DOI Android application, the user's name, Google username, Gmail address or other personal information provided by the user may become available to DOI and other Google users. DOI will use this information as needed, but will not otherwise request or collect PII.

Other Uses of PII

Except as described above, DOI will not collect or share PII through its use of Android applications, except in unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, Google username, Gmail address, and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

2.2 What are the sources of the PII?

Sources of PII are Android application users world-wide, including members of the general public and Federal employees, and may include other government agencies and private organizations.

2.3 Will the PII be collected and maintained by the agency?

PII may become available through interactions with Android device users. If an Android device user interacts with DOI through the use of a DOI Android application, requests information, submits feedback or rates a DOI Android application, their name, Google username, Gmail address or other personal information provided by the user may

become available to DOI. DOI will not share PII from the use of Android applications, except in unusual circumstances where there is evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, Google username, Gmail address, and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

Certain applications will collect geolocation information independent of any other types of PII. DOI will maintain and use this information in keeping with our agency mission objectives as needed. The data may be released to the public, but will only be done in an anonymous, aggregated fashion that will prevent the personal identification of individuals.

With certain applications, a limited amount of contact information will be collected from users to facilitate follow up communications. This will only be done with the user's knowledge and consent, when doing so will provide a benefit to the individual being contacted or the public as a whole, or otherwise furthers DOI's mission. The contact data will be maintained on Google's servers, and will only be accessed if follow up communication is desired by DOI. Contact information will be maintained by DOI or Google only for a reasonable period of time in which to initiate contact with the user.

Any DOI bureau or office that uses an Android application that creates additional privacy risks must complete a separate PIA for the specific use and collection of information, and must maintain any PII collected in accordance with DOI-08, Social Networks system of records notice, or applicable bureau or office system of records notice as appropriate. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/index.cfm.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

Each Android application that is created will be reviewed by the Information Collection Clearance Office for the bureau or office that will use the application. In the event that use of an application triggers the PRA, an Information Collection Clearance Collection request will be prepared and submitted to the Office of Management and Budget (OMB).

SECTION 3: The Agency's Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

PII may become available through interactions with Android device users. If an Android device user interacts with DOI through the use of an Android application, requests information, submits feedback or rates a DOI Android application, their name, Google username, Gmail address or other personal information provided by the user may become available to DOI and may be used by DOI to provide a response.

The Department will not share PII from the use of Android applications, except in unusual circumstances where there is evidence of criminal activity, a threat to the

government, a threat to the public, or an employee violation of DOI policy. This information may include name, Google username, Gmail address, and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

Certain applications will collect geolocation information independent of any other types of PII. DOI will maintain and use this information in keeping with our agency mission objectives as needed. The data may be released to the public, but will only be done in an anonymous, aggregated fashion that will prevent the personal identification of individuals.

With other applications, a limited amount of contact information will be collected from users to facilitate follow up communications. Contact information will be utilized by DOI when doing so will provide a benefit to the individual being contacted or the public as a whole, or otherwise furthers DOI's mission. Contact information will be maintained by DOI only for a reasonable period of time in which to initiate contact with the user in accordance with applicable records retention schedules.

3.2 Provide specific examples of the types of uses to which PII may be subject.

If an Android device user or member of the public interacts with DOI through the use of an Android application, requests information, submits feedback or rates a DOI Android application, their name, Google username, Gmail address or other personal information provided by the user may become available to DOI. DOI will not share PII from the use of Android applications, except in unusual circumstances where there is evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, Google username, Gmail address, and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

In certain applications, a limited amount of contact information will be collected from users to facilitate follow up communications. This will only be done with the user's knowledge and consent, when doing so will provide a benefit to the individual being contacted or the public as a whole, or otherwise furthers DOI's missions. The contact data will be maintained on Google's servers, and will only be accessed if follow up communication is desired. Contact information will be maintained by DOI or Google only for a reasonable period of time in which to initiate contact.

SECTION 4: Sharing or Disclosure of PII

4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

DOI will not share PII with entities or persons outside of DOI. However, there may be cases where there is evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, Google username, Gmail address, and other personal information provided by the user,

and may be used to notify the appropriate agency officials or law enforcement organizations.

Certain applications will collect geolocation information independent of any other types of PII. DOI will use this information in keeping with our agency mission objectives as needed. The data collected may be released to the public, but will only be done in an anonymous, aggregated fashion that will prevent the personal identification of individuals.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

Some of DOI's Android applications may permit users to submit questions or comments to DOI through private communications tools such as instant messaging or email. In addition, users may be asked to provide contact information in order to facilitate follow up communications. Any private communications or contact information will only be available to appropriate DOI officials and will not be accessible to other application users. All PII obtained from DOI's Android applications will be held in password protected Google accounts that will only be accessible by authorized DOI personnel.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

PII that is a part of a Federal record will be retained in accordance with the applicable record retention schedule. Retention periods vary as records in each Android application are maintained in accordance with the applicable records schedule for each specific type of record maintained by the Department. Records published through DOI Android applications, such as publications through the content delivery applications described above, represent public informational releases by the Department, and must be assessed on a case-by-case basis depending on the individual/entity releasing the information and the purpose of the release. There is no single records schedule that covers all informational releases to the public at this time.

Comments and input from the public, including data received through DOI's scientific data collection Android applications, must be assessed by whether it contributes to decisions or actions made by the government. In such cases where input from the public serves a supporting role, the comments must be preserved as supporting documentation for the decision made.

PII that is not part of a Federal record subject to the National Archive and Records Administration (NARA) retention requirements will be retained as needed, then promptly destroyed. Approved methods for disposition of records include shredding, burning, tearing, and degaussing in accordance with NARA guidelines and 384 Departmental Manual 1.

5.2 Was the retention period established to minimize privacy risk?

Retention periods may vary depending on agency requirements and the subject of the records for the DOI bureau or office maintaining the records. In cases where data serves to support agency business, it must be filed with the pertinent records they support and follow the corresponding disposition instructions. Comments used as supporting documentation will utilize the disposition instructions of the records they are filed with. PII that is not part of a Federal record subject to NARA retention requirements will be retained as needed, and promptly destroyed.

SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Yes. Privacy and security officials work with the Office of Communications and bureau and office personnel to develop methods for protecting individual privacy and securing PII that becomes available to DOI through the use of Android Developer applications.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

Any PII maintained by DOI is secured in accordance with DOI Privacy Act regulations 43 CFR Part 2 and applicable DOI privacy and security policies. Access to the DOI network is restricted to authorized users with password authentication controls, servers are located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on official need to know. Other security controls include continuously monitoring threats, rapid response to incidents, and mandatory employee security and privacy training.

In certain applications, a limited amount of contact information will be collected from users to facilitate follow up communications. Contact information will be utilized by DOI when doing so will provide a benefit to the individual being contacted or the public as a whole, or otherwise furthers DOI's mission. Contact information will be maintained by DOI only for a reasonable period of time in which to initiate contact with the user in accordance with applicable records retention schedules. Any private communications or contact information will only be available to authorized DOI officials and will not be accessible to other application users. All PII obtained from DOI's Android applications will be held in DOI Google accounts that are password protected and will only be accessed by authorized personnel.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

Mobile Device Risks

Mobile devices present an enhanced privacy risk, including:

- ***Loss of device.*** Mobile devices are small, portable devices that are regularly used and carried in public places. As a result, there is a significant risk of loss or theft. Mobile users can protect against unauthorized access to data in the event of loss or theft by using mobile device password protection.

- ***Use of unsecured Wi-Fi networks.*** As a matter of convenience, many mobile device users connect (either occasionally or frequently) to the Internet via unsecured Wi-Fi networks. Signals transmitted over such networks are often unencrypted, creating a risk that data being transmitted over the network can be viewed by other users. Users can choose to connect to the Internet through secured Wi-Fi connections or secured mobile networks available through cellular providers instead. For those who choose to use unsecured Wi-Fi connections, the risks can be mitigated through various device settings and applications, such as firewalls or other restrictions on external access to a device.

- ***Geolocation.*** Many mobile devices include GPS chips that calculate the precise geographic location of the device. This location information is available to applications installed on the mobile device and may be transmitted to third parties, providing both real time and historical information about a user's physical location. The sharing of geolocation data can be prevented by turning off GPS location on the mobile device or by adjusting settings to prevent sharing of location information with third parties.

While mobile devices present increased privacy risks, the creation and distribution of Android applications by DOI is not likely to materially impact mobile users' privacy because DOI Android applications will not result in additional personal information being collected on users' mobile devices. Nor will there be a significant increase in users' personal information being held by Google as the PII that is collected and used by DOI Android applications is already on the device and already held and maintained by Google.

While it may be possible for users to send personal information to DOI through DOI's Android applications through email or instant messaging tools, it is not anticipated that a large volume of personal information will be shared with DOI in this manner. It is even less likely that users will submit personal information to DOI through a mobile application under circumstances where privacy might be compromised.

The risks described above are generally applicable to the use of mobile devices, and the addition of applications to the Android marketplace by DOI is not expected to have any impact on Android users' decisions to take (or not take) certain protective steps such as implementing mobile device password protection or exercising caution concerning the use of Wi-Fi networks.

Geolocation Concerns

DOI will utilize a tiered approach to address and minimize the privacy impacts resulting from the use of geolocation APIs.

1) **Geolocation data maintained and processed on Google's servers; DOI does not obtain user geolocation data.** In certain cases, DOI will use geolocation data to provide enhanced information to users. An example of this is a self-guided tour of a historical site using location-dependant program variables processed on Google's infrastructure. In these cases, specific location information will be obtained from a user's device by a specific geolocation API, and processed and held by Google. Data placed on Google's servers, including text, images, audio, or video specific to predefined GPS coordinates will be delivered to the user by Google based on a user's location, and DOI will not see the user's specific location.

2) **Geolocation data collected independent of other forms of PII; DOI receives geolocation data without any additional information to identify users.** Where geolocation information collection or processing by DOI is necessary for the functioning of an application, the Department will endeavor to collect the geolocation information independently from any other PII. Geolocation information will be collected and utilized by DOI, but will not be collected with any other PII, such as name or contact information.

3) **Geolocation data collected by DOI along with other PII; DOI will provide clear notice of the collection of information and the purpose of collection, along with the option to submit data anonymously.** Where geolocation data is collected with other forms of PII, DOI will notify the user of the purpose of collecting the additional PII and, where feasible, provide the option not to submit additional PII. Users will be provided notice upon the initialization of the application, as well as every instance in which data is submitted. When appropriate, users will have the option to submit information without providing contact information.

In order to further minimize any privacy risks associated with geolocation data, DOI will abide by the following guidelines with respect to any DOI Android applications that collect geolocation information:

- Any application that collects geolocation information will contain a Terms of Service for users to read and assent to prior to initializing the application. The potential collection of geolocation information will be disclosed, along with a description of how the information will be used.

- Geolocation information and any affiliated PII will be used only in accordance with the purpose as stated in DOI Terms of Service and Privacy Notice.

- Geolocation information and any related data will be promptly deleted when it is no longer needed for the purpose for which it was collected in accordance with applicable records retention requirements.

Viruses and Malware

Android applications are written in the Java programming language; completed applications are downloaded and installed to a user's Android device. For security purposes, each Android application operates in isolation from other applications and does not share application code. Furthermore, the Android operating system runs applications using the principle of least privilege; each application, by default, has access only to the components needed to run properly. This increases operating environment security and minimizes the opportunity for viruses, malware or system errors.

Nevertheless, all software, including Java software, is at risk for viruses and malware, including malware that can be used to steal personal information. DOI cannot guaranty the security of the Android operating system or the security of the Google APIs used in DOI Android applications; Android is a third party operating system, and Google, as the owner of Android, is responsible for ensuring the security of the APIs it makes available to developers.

Personal information provided by users of DOI Android applications is expected to be minimal, in terms of volume, scope and level of sensitivity. As a result, even if a DOI Android application is installed on a device that contains malware, the types of PII obtained by DOI Android applications is not expected to present a significant privacy risk.

7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of third-party website or application?

Use of each DOI Android application will require acceptance to Terms of Service and a Privacy Notice in order to complete the installation of the application on their mobile device. The Terms of Service will inform the user of the potential collection of information and how that information will be used, and user consent to the terms will be logged in the application database held by Google.

The Privacy Notice will inform users as to how DOI handles PII that becomes available through user interaction, and directs Android application users to the DOI Privacy Policy for information handling practices. DOI's Privacy Policy informs the public of how DOI handles PII that becomes available through interaction on the DOI official website. The Privacy Policy also informs the public that DOI has no control over access restrictions or privacy procedures on third party websites, and that individuals are subject to third party website privacy and security policies. DOI's linking policy informs the public that they are subject to third party privacy policies when they leave a DOI official website to link to third party websites.

SECTION 8: Creation or Modification of a System of Records

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

The purpose of developing DOI Android applications is to make full use of mobile technologies in the dissemination of information to the public, and to enhance communication, promote public participation and collaboration, and increase government transparency in support of the Administration's initiative to build a 21st century digital government, and provide more efficient and coordinated digital service delivery. DOI will generally not collect, maintain or disseminate PII through the use of Android applications in any way that creates or modifies a system of records. However, PII may become available through interactions with Android device users. Any DOI bureau or office that develops or uses an Android application in a way that creates a system of records must complete a separate PIA for that specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks system of records notice, or other applicable bureau or office system of records notice as appropriate. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

8.2 Provide the name and identifier for the Privacy Act system of records.

DOI will generally not collect, maintain or disseminate PII through the use of Android applications in any way that creates a system of records. However, PII may become available through interactions with Android device users. Any DOI bureau or office that develops or uses an Android application in a way that creates a system of records must complete a separate PIA for that specific use and must maintain the records in accordance with DOI-08, Social Networks system of records notice, or other applicable bureau or office system of records notice as appropriate. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.